PV8

April 17, 2020

The Honorable Paul A. Crotty
United States District Judge
Southern District of New York
United States Courthouse
500 Pearl Street
New York, New York 10007

RE: United States v. Joshua Adam Schulte, S2 17 Cr. 548 (PAC)

Dear Judge Crotty:

As the Court is aware, I have invoked my right to a speedy trial guaranteed by the Sixth Amendment. Since I have no counsel and currently not granted bail, it seems this case will drag on for decades unless I invoke my Sixth Amendment — and since I have been tortured in solitary confinement for over 18 months — there is little choice. The speedy trial clock has been ticking since my hung jury on 3/9/2020 and only a few months now remain.

In order to properly defend myself, I move to compel the Government to produce missing discovery pursuant to Rule 16; I move for an order to return seized devices pursuant to Rule 41(g); I move to compel the production of a modern useable laptop with digital law library software; I move for an injunction to compel MCC to provide phone calls with my family; Finally, I move for an injunction to compel MCC to deliver legal mail in a prompt and timely manner.

P.2

A. Motion to Compel production of discovery pursuant to Rule 16

1. Production of decrypted Plex Server, QNY_56_SC48_SRV01

The Government should be compelled to produce to me a decrypted forensic image of the Plex Server. To date, the Government has only produced this server in a decrypted format to the Federal Defenders, but not to me at MCC. It has previously been requested, but the Government has simply ignored requests since at least August 2019. Since this forensic image is extremely large, the Government need only produce an external drive with the raw, decrypted image (not FTK files or other processed data) and a forensic write blocker. This server is the basis for Count 15 - Copyright infringement. Without this server, I cannot defend myself on Count 15 and will move to dismiss this count if the Government does not produce this forensic image to me in a prompt and timely manner.

2. Production of Windows Hyper-V Server, QNY_56_SC48_SRV02

The Government should be compelled to produce to me the Hyper-V Server and all virtual machines. To date, the Government has not produced this server to the Federal Defenders nor to me. This server and its associated VMs do not contain any child pornography according to the Government (only QNY09_SC01_desktop). The "classified" information stored on this server were the publicly released Snowden documents viewed from a web browser. It would be absurd for the Government to classify every defendant's computer that was used to view publicly released documents available on the internet and it's absurd here. The Government never showed these Snowden documents to the jury, produced them as exhibits, or even alleged any illegal activity regarding these documents. This server is critical to all Counts of the indictment and the Government should be compelled to produce it.

3. Partial image of QNYØ9_SCØ1_Desktop

The Government should be compelled to produce a partial image of QNYØ9-SCØ1_Desktop. The only child pornography on this Computer is self-contained within a single file – a VirtualBox VM. The Government should produce a forensic image of this system without that single file – which is trivial to do. In fact, the Government did just this when they produced partial images of my CIA workstation and the Confluence backup files; they removed all the files they deemed as "too classified" to produce in classified discovery. For the QNYØ9_SCØ1 forensic image, they need only remove a single file instead of millions. The Government should be compelled to employ this trivial technique to remove the single CP VM from the forensic image and produce that image to me. Without a forensic image of this system, I cannot defend the three CP counts and will move to dismiss those counts.

4. Complete forensic images of DEVLAN

The Government should be compelled to produce the forensic images of the CIA's ESXi server, FSØ1 server, and my CIA workstation. Without the digital crime scene, I cannot defend myself against the espionage counts and will move to dismiss them.

—SEE EXHIBIT A—

B. Motion for return of seized electronics pursuant to Rule 41(G)

The Government should return non-responsive and irrelevant devices to my family in Texas; Non-responsive, irrelevant devices that were never even imaged; Non-responsive, irrelevant devices that were imaged but are immaterial; And finally non-responsive, irrelevant, and blank devices. The only three electronic devices the Government should retain are the Rack Server and drives (1B56) and Black Tower Computer (1B55).

1. Return of non-responsive, irrelevant items that were never even imaged

Several items seized from my residence were not responsive to the Search Warrants and were not even imaged or produced to the defense. Those items should be returned to my family in Texas

a. 1B39 One TP-Link Network USB
b. 1B38 One Garmin Nuvi S/N 1CZ041768
c. 1B36 One MS Zune MP3 Player S/N 014195164210
d. 1B35 One Olympus Camera JOH244018
e. 1B18 One Kindle
f. 1B16 One Kindle
g. 1B15 One XBOX 1 S/N 149212254048
h. 1B14 One XBOX 360 S/N 033320322443
i. 1B13 One SanDisk MP3 Player
j. 1B12 One SanDisk MP3 Player

These 10 items were never even produced in discovery, are not responsive to the SWs, and are entirely irrelevant to the case. All items should be returned pursuant to Rule 41(G)

2. Return of non-responsive, irrelevant items that were imaged

Several items seized from my residence were not responsive to the search warrants and were forensically imaged. These irrelevant items should be returned to my family in Texas

a. 1B54 One Bag Containing 7 CD/DVDs
b. 1B53 One Bag Containing 27 CD/DVDs
c. 1B52 One Bag Containing 28 CD/DVDs
d. 1B51 One Bag Containing 29 CD/DVDs
e. 1B50 One Bag Containing 15 CD/DVDs
f. 1B49 One Bag Containing 9 floppy disks & 5 CD/DVDs
g. 1B48 One ATT Sim Card
h. 1B47 One 16 GB MicroSD
i. 1B46 One 8GB SanDisk MicroSD
j. 1B45 One UFCU 128 MB TD
K. 1B44 One SANS TD
l. 1B43 One SanDisk 16B TD
m. 1B42 One PNY 16B TD
n. 1B41 One OSR TD
o. 1B40 One SanDisk USB TD 16GB
p. 1B37 One HTC Phone S/N HTB06GØØ19Ø1
q. 1B34 One HTC Phone S/N HTO68P9ØØ155
r. 1B33 One Samsung Phone Model SPHL71Ø
s. 1B19 One Samsung Phone model SM-J32ØP
t. 1B17 One Samsung Tablet S/N R52H6ØLF5RY
u. 1B10 One SanDisk TD
v. 1B9 One Black Server Tower

3. Return of non-responsive blank and irrelevant hard drives

All blank hard drives or hard drives and computers not responsive to the Search Warrants should be returned. Drives that are all zero cannot possibly be responsive by definition since they literally contain no data. All computers and hard drives that the Government does not intend to use at trial or which do not contain any evidence of the charged Criminal activity should also be returned.

C. Motion to compel production of modern laptop for discovery review

The Government should be compelled to produce a modern Windows 10 laptop with modern average processing power and at least 8 hours of battery life with digital law library capability so that I can at least attempt to defend myself. The current laptop produced by the Government is insufficient because it is a decade old and only permits an hour of use even with the new battery the Government purchased to address this problem. This laptop was sufficient when I was in General Population because I could simply plug it in but on SAMs I cannot use power outlets and therefore only get an hour use — 30 minutes when I'm using the external discovery drive — and I only get one charge per day. Since I am on SAMs and cannot use a power outlet, the Court should compel the Government to purchase a new, modern laptop for my use. Besides, the Government forced me to purchase a laptop for the classified discovery that Dan Hartunstine the CSO said I should not have had to purchase — the Government was supposed to purchase it through Dan. So, the Government owes me a laptop anyway. Finally, the Government should also be compelled to provide the electronic law library software that they purchase and use, such as Westlaw, LexisNexis, etc. Again, since I am on SAMs I am not permitted use of the Institution's library. To compensate and provide me equal access to the Government's resources, the Government should provide me the same software

D. Motion for injunction to compel MCC to provide SAMs inmates family calls

BOP Director M.D. Carvajal ordered the BOP to increase inmate's monthly phone minutes and provide free phone calls to inmates to compensate for the cancellation of all visits. This new policy went into effect April 9, 2020, but MCC has not applied this to SAMs inmates; In fact, we get no phone calls as well as no visits. I have not seen or spoken to my family since my February trial. If the BOP is going to suspend all visits and give all other inmates extra minutes and free phone calls, this Court should order it applied to SAMs inmates as well.

E. Motion for injunction to compel MCC to deliver legal mail promptly

Due to SAMs, MCC does not deliver any mail for several months. Court correspondence — with this Court, the Court of Appeals, and even the Supreme Court must be screened first by the FBI before delivery. This causes unnecessary delay & causes me to miss deadlines. There is no reason the FBI needs to read mail sent to me from the Court and no reason the MCC needs to sit on mail for months after the screening. To ensure due process, this Court should compel MCC to forego FBI screening of all Court correspondence and legal mail sent to me, and order the MCC to deliver all Court correspondence and legal mail in a prompt, timely manner.

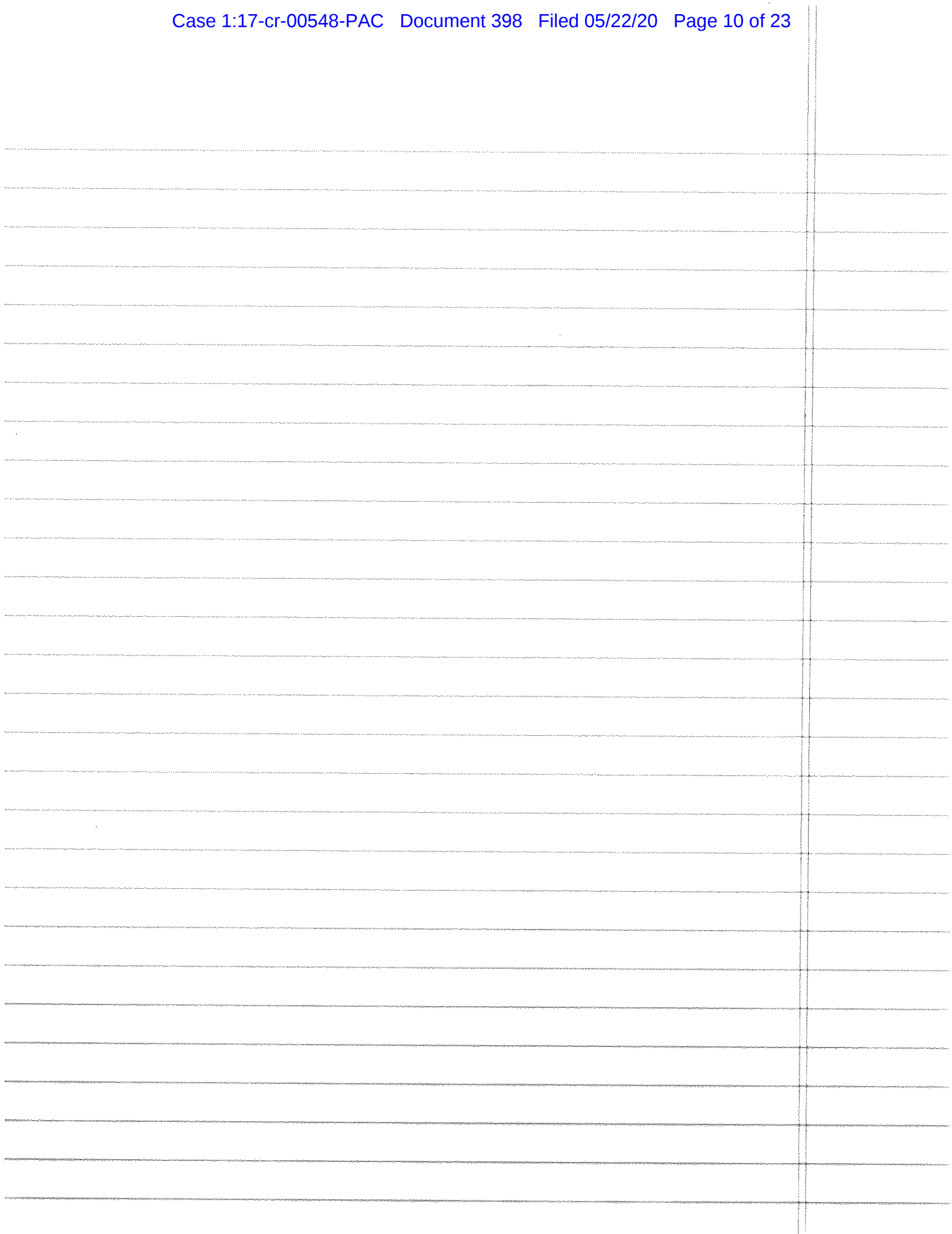
F. Summary

For the reasons described herein, this Court should order and compel the Government to produce missing discovery pursuant to Rule 16, order the Government to return all non-responsive and irrelevant electronics pursuant to Rule 41(g), order and compel the Government to provide me a modern laptop with at least 8 hours of battery life and law library software, order and compel the MCC to follow the BOP's executive decision for SAMs inmates, and finally, order and compel the MCC to forego FBI screening for Court correspondence and legal mail sent to me and to deliver it promptly.

Josh Schulte

4/12/2020 Josh Schulte

EXHIBIT A



4/12/20

~~September 30, 2019~~

Hon. Paul A. Crotty
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: *United States* v. *Joshua Adam Schulte*, S1 17 Cr. 548 (PAC)

Honorable Judge Crotty:

The defense renews its request for the Government to produce the crime scene forensic images in this case—the complete forensic images from the computer systems alleged by the Government to be the epicenter of the espionage charges against Mr. Schulte. Specifically, the Government alleges that the defendant committed the espionage offenses by accessing a virtual machine on the ESXi server remotely from his CIA workstation and exfiltrating data from the backup server. Hence, the CIA workstation, ESXi server, and backup server are paramount to this case; none have been fully produced to the defendant.

~~Trial is scheduled in three months, but~~ the Government has failed to provide the forensic images from these three computers or even the specific backup files or other data allegedly stolen from the CIA. The forensic images are proper Rule 16 and even Brady; in every computer-crime case that we've reviewed in both state and federal courts, forensic images have been consistently considered relevant and disclosed to the defense—in no case has a prosecutor ever argued, let alone a judge ruled, that the forensic images from an alleged digital crime scene were "not relevant" to the defense.

The forensic images are imperative not only because denying them to a defendant would be unprecedented, but also because it is impossible for any technical or forensics expert to request specific files without conducting a forensic review and knowing which files even exist; the Government itself has made extensive use of the forensic images and created demos which the defense cannot validate or rebut without similar access; the complexity of the case and multiple months of review by the Government prior to even deciding to prosecute illustrate the defense's need for equal access to the information; the evidence provided thus far show the Government compromised the integrity of the servers during its analysis; existence of classified information on the servers does not make the forensic images irrelevant nor does it override the 6th amendment; the complete lack of information given to the defense would necessarily introduce reasonable doubt and provoke an argument for jury nullification; finally, the images are necessary to put on a defense as guaranteed by the 6th amendment.

A. Forensic images have always been considered relevant in cases of computer crimes

There is not a single case in state or federal criminal court in which a defendant accused of computer crimes was not given a forensic image of the very computers involved in the crime. In fact, every prosecutor has conceded that forensic images are relevant and have never before required the defense to *specify* files from a forensic image that the defense has never reviewed. Put simply, the forensic images are relevant because they constitute the crime scene. They are relevant, Rule 16 material and have always been since the first charged computer crime. Thus the Government's argument otherwise is unprecedented and unpersuasive.

Furthermore, the prosecutors themselves are not in any position to deny forensic images because they do not have direct knowledge of the forensic images, but are simply relying on technical experts. Since they have not conducted the forensic reviews nor do they even understand the basics, how can they be sure that within these tens of *trillions* of bytes there isn't something relevant and helpful to the defense? How is it they get to review those bytes, pick out what they want to introduce at trial, and then deny this same review to the defense—instead claiming the very evidence they reviewed is "not relevant" and the defense should be required to request what files they want when they don't even know what files exist? It's beyond absurd. If the prosecutors are wrong, or rather, if their forensic experts missed something—who would ever know? Data is easily overlooked by a team that doesn't want to find Brady material, is not familiar with the computer systems, and who are content in their confirmation bias. This is why the defendant has counsel and the ability to hire his *own experts* to review the evidence to put on a defense—if every trial simply deferred to the Government's analysis there would be no more trials. A decision to deny forensic images to defendants in cases of computer crimes would completely eradicate all trials for computer-related crimes.

B. It is impossible to request specific files without a proper forensic analysis

It is impossible for the defense to request specific files without conducting a forensic review. No technical expert or forensics expert can possibly defend allegations of wrongdoing without reviewing and conducting analysis themselves on the forensic images. No expert could possibly know what files are helpful to the defense without review.

The Government has even refused to list the names of files on the machines or other associated metadata. But even with this information, a technical expert could still only speculate what files may or may not be useful. If information was stored on the machine in an atypical manner or data was hidden then the technical expert would have no idea to request for this information. Additionally, due to file slack space, volume slack space, and unallocated/free space, as well as stegonagraphy and intentional data hiding techniques, some

data is not contained within the files themselves but exist only in areas of the disk reviewable through forensic analysis alone.

Additionally, the Government has produced a forensic image of the defendant's CIA workstation to the defense. However, recently the defense learned through its analysis that this forensic image is incomplete; the forensic image was purposefully modified by the Government to delete files, programs, and folders from review. The resulting forensic analysis is incredibly misleading as the holes in the forensics create misinformation and lead the analyst to faulty conclusions about the data. After requests for the missing data, the Government produced a partial file listing—which is far from sufficient. Also note that two years ago the defense requested forensic images of the defendant's servers with the alleged classified information removed from the image, but the Government claimed it could not do this because it did not have the "technology" to do so. Here, however, the Government produced forensic images in classified production where they were able to remove information that they did not want the defense to see, in stark contrast to their original claim that this was impossible (The Government has still, after two years, failed to produce forensic images of the defendant's home servers in either classified or unclassified discovery).

C. The Government itself has made extensive use of the forensic images and has used them to create demonstrative videos that the defense cannot reproduce, validate, or rebut without equal access

The Government has used the forensic images to produce multiple demonstrative videos that they intend to produce at trial of "reenactments" of how they speculate the data was stolen. These videos involve the Government logging into, accessing, and otherwise interacting with the servers at the forefront of this case. Since the defense does not have access to these servers, we cannot validate the Government's theory, reproduce the Government's videos, or produce demonstrative videos of our own showing the defense's theory of what happened. Instead, the Government has created a scenario in which the defense cannot reply to its argument. This is unprecedented and in clear violation of the 6th amendment.

D. Complexity

The complexity of this case is such that law enforcement and the CIA spent 15 months, thousands of people, and millions of dollars reviewing, re-reviewing, analyzing, and re-analyzing the forensic images and other data in this case before deciding to prosecute. The defense will never have access to the incredible resources of the United States Government, but should at least have access to the same forensic data the Government reviewed. The reason this has taken so long is the case involves tens of *trillions* of bytes of very complicated data—data that could easily be overlooked by the Government's analysts.

Also note the Government's prosecution theory is entirely a consciousness-of-guilt circumstantial case. The Government does not have a single piece of evidence showing what information was taken from the CIA, how it was taken, where it was taken from, or even how and when it was given to Wikileaks. The Government's entire theory is built around anomalous data located in unallocated, undefined space—evidence the Government will claim shows the deletion of log files—but of course not the content of what was deleted or why. The Government will argue it was the defendant who deleted the log files and that this shows consciousness-of-guilt and therefore the defendant committed a crime. Thus, the Government will ask the jury not only to take the leap of faith to believe that the defendant deleted log files, but also that those log files would have shown something that would have been circumstantial and somehow related to the theft of the data. No case like this has ever been tried—and a man's life hangs in the balance. It is critical to ensure the defense has the same tools as the Government and can adequately prepare its case.

E. The provided files from the ESXi server show that the Government modified the forensic image in its review, thereby damaging the integrity of the data and necessitating suppression due to spoliation if they did not keep the original data intact

Data integrity is another very important issue here. Since the defense cannot review the forensic images then how is the data integrity ensured? Without fully intact forensic images, the defense cannot verify whether the data the Government presents is the data they claim it is—or from where they claim it's from. For example, DNA evidence that's been compromised is inadmissible at trial—so is forensic evidence that's been compromised. From the few files that the Government has turned over to the defense, it appears that the Government did not follow proper procedures when conducting its forensic examination (similar to proper procedures in analyzing DNA samples). Hence, the resulting evidence is compromised and potentially inadmissible in court. However, the defense cannot file a spoliation motion with only one file—we need the entire forensic images for our expert to testify that the data's integrity was compromised during the Government's sloppy review.

F. Existence of Classified Information on the forensic images do not preclude the image's relevance or override the 6th amendment

The Government's true reason for refusing the defense's review is the classified information on the forensic images. The fact that the forensic evidence contains classified information is unfortunate, but there is no way to disentangle this classified information in digital format. It is not simply a matter of sorting papers and taking out or redacting information in paper copy. The crime scene itself is imprinted across these servers and mingled in every way. In fact, the deleted space and other data that is intertwined with the files and the very property of digital information make it paramount for analysis on the full forensic images.

The CIA and the Government cannot have their cake and eat it too—they cannot conceal crime scene evidence simply because it is classified while accusing the defendant of committing a crime on the classified servers, but refusing the defense from reviewing this evidence; the fact that the forensic images are classified simply do not detract their relevance under Rule 16 or overrule the 6th amendment.

Additionally, this is exactly why defense counsel must undergo the rigorous clearance process to obtain security clearance—so they can view the classified information. In fact, if the prosecutors receive clearance and are granted the need-to-know then it's only fair that defense counsel is granted the same clearance and access. To do otherwise would simply violate the 6th amendment and guarantee that the trial is not fair. And finally, all the classified information in this case has either been published publicly or according to counter-intelligence protocol, must be considered compromised anyway; the CIA is not launching any operations with the data exposed in this breach—so why can't cleared defense counsel view it?

A ruling that forensic images of crime scenes in digital cases are not relevant would be a slippery slope and open Pandora 's Box—could banks and other financial institutions that are hacked then claim that the digital forensics aren't relevant in these criminal cases as well because the information is sensitive financial information? Could every victim refuse defense the ability to review forensic evidence simply because they claim it's sensitive and "not relevant"? Any ruling rejecting the defense's request for forensic images would be devastating and end all trials in computer crime cases since the defendants would be at an overwhelming disadvantage.

G. The Government's failure to disclose the forensic images necessarily introduces reasonable doubt and provokes jury nullification in the expert and defendant's testimony

At trial this issue will come into play as jury nullification when both the technical expert and defendant explain and show numerous potential theories, but say "we were not given the evidence for review to confirm or reject these hypotheses." This necessarily introduces reasonable doubt and provokes an argument for jury nullification. There is no way to stop this testimony because the defense has a 6th amendment right to put on a defense—but here the defense was not permitted to review the evidence so the defense will simply say the Government would not turn over the forensic evidence so we cannot put on any defense. The defense cannot even verify most of the Government's assertions, let alone put on a defense itself. The result, even if unspoken, remains clear: What American wants to be accused of a crime and not given the evidence to review? If any juror is appalled and would not want to have a trial without the chance to review the full evidence then they must acquit, regardless of all

other factors. This is the point of jury nullification—to provide a check by the People against Government tyranny and oppression.

H. It is unprecedented to deny a defendant review of the crime scene

It is clearly absurd if the Government refused to turn over all fingerprints found at a crime scene—if they said no this isn't relevant; WE don't intend to present this at trial so it's "not relevant". Or if the Government refused to allow the defense to hire its own experts to rebut the Government's experts—if the Government said no, our expert will testify so it isn't necessary for you to hire one. There is absolutely no difference between this and what the Government is doing—only in digital space. The defendant is not merely relegated to countering the Government's presented evidence—but to also review and put forth his own evidence and his own theory. To deprive a defendant from review of the crime scene is un-American, unprecedented, unjust, and clearly repugnant to the 6th amendment.

I. Conclusion

Despite the Government's initial search warrant on March 13, 2017 and its targeting of the defendant in the Wikileaks case, it took them 15 months of analyzing and processing the forensic crime scene before deciding to prosecute the defendant in June 2018. Since then, the Government has had an additional 15 months to rework and hone their theories while simultaneously denying the defense equal access. The idea that the Government can review and process the crime scene data and the defense cannot is repugnant to the 6th amendment and the notion of a fair trial. The 6th amendment and guarantee of a fair trial is inherent in the founding of the country. Prior to our declaration of independence and constitutional rights to a fair trial, those accused of treason or crimes against the Crown—if they even received a trial at all—were forbidden counsel, not permitted to call witnesses, and not even allowed secretaries to help prepare their case; in essence, the all-powerful monarch was judge, jury, and executioner. The United States Government has taken us back to the Dark Ages and this dangerous principle of denying those accused of crimes against the State from access to evidence or the ability to put on a defense.

In conclusion, the defense renews its request for the same full access to the digital crime scene as the Government to prepare a defense before trial.

Park Row
k, NY 10007

ATTN: Criminal Case S2 17 Cr. 548 (PAC)
Hon. Paul A. Crotty
United States District Judge
Southern District of New York
United States Courthouse
500 Pearl Street
New York, NY 10007